1 <!--->

Rules

- Android Security Rewards Program Rules
- Chrome Vulnerability Reward Program Rules
- Developer Data Protection Reward Program Rules
- Google and Alphabet Vulnerability Reward Program (VRP) Rules
- Google Play Security Reward Program Rules
- Open-source Security Subsidies Rules
- Our Rewards Philosophy
- Patch Rewards Program Rules
- Research Paper Rewards Program Rules
- Vulnerability Research Grant Rules

Android Security Rewards Program Rules

The Android Security Rewards program recognizes the contributions of security researchers who invest their time and effort in helping us make Android more secure. Through this program, we provide monetary rewards and public recognition for vulnerabilities disclosed to the Android Security Team. The reward level is based on the bug severity and increases for complete reports that include a high-quality, buildable proof of concept that reproduces against a recent build of Android (no older than 30 days at time of submission).

Scope of program

Pixel phones and tablets. This set of devices changes over time, but as of October 19, 2021 this covers:

- Pixel 6 and Pixel 6 Pro
- Pixel 5
- Pixel 4a 5G
- Pixel 4a
- Pixel 4 and Pixel 4 XL
- Pixel 3a and Pixel 3a XL

Android Security Rewards cover bugs in code that run on eligible devices and aren't already covered by other reward programs at Google. Eligible bugs include those in AOSP code, OEM code (libraries and drivers), the kernel, the Secure Element code, and the TrustZone OS and modules. Vulnerabilities in other non-Android code, such as the code that runs in chipset firmware, may be eligible if they impact the security of the Android OS.

- Vulnerabilities in applications developed by Google and published in Google Play (e.g., Maps) should be reported to the Google VRP which also covers server-side issues.
- Vulnerabilities in Chrome should be reported to the Chrome Rewards program.
- Vulnerabilities in popular third-party Android applications should be reported to the Google Play Security Rewards program.

At this time, vulnerabilities that only affect other Google devices (such as Android Wear or Project Tango) are not eligible for Android Security Rewards.

Qualifying exploit chains

We provide an extra reward for a full exploit chain (typically multiple vulnerabilities chained together) that demonstrates arbitrary code execution, data exfiltration, or a lockscreen bypass. The actual reward amount is at the discretion of the rewards committee and depends on a number of factors, including (but not limited to):

- The initial attack vector (i.e. remote exploitation versus local).
- Whether the exploit is device- or build-specific, or whether it works across a broad set of builds and devices.
- The amount of user interaction required for the exploit to work.
- Whether the user could feasibly detect that an exploit is in progress or has completed.
- How reliable the exploit is.
- Exploit chains found on specific developer preview versions of Android are eligible for up to an additional 50% reward bonus.

Maximum exploit rewards for each type of exploit are listed below:

Code execution reward amounts

Description	Maximum Reward
Pixel Titan M	Up to $1,000,000
Secure Element	Up to $250,000
Trusted Execution Environment	Up to $250,000
Kernel	Up to $250,000
Privileged Process	Up to $100,000

See Process types for category descriptions.

Data exfiltration reward amounts

Description	Maximum Reward
High value data secured by Pixel Titan M	Up to $500,000
High value data secured by a Secure Element	Up to $250,000

Bypass reward amounts

Lockscreen bypass [1]	Up to $100,000
Device Policy Controller bypass [2]	Up to $75,000

[1] This reward is applicable to lockscreen bypass exploits achieved via software that would affect multiple or all devices. Spoofing attacks that use synthetic biometric data (fake masks, fingerprints, etc.) are not eligible for reward.

[2] This reward is applicable to exploits that remove the Device Policy Controller as the admin from a fully managed device.

Qualifying vulnerabilities

We also reward individual vulnerabilities (for example, a single bug demonstrating memory corruption or permissions bypass) that have a security impact.

In general, we reward critical, high, moderate, and low severity vulnerabilities. Patches that don't necessarily fix a vulnerability, but provide additional hardening may qualify for Google Patch Rewards.

There are a few rules that we follow when rewarding a vulnerability report:

- A bug report should include as much detail as possible, a buildable proof of concept against a recent build (no older than 30 days at time of submission), a crash dump if available, and any additional repro steps. For tips on how to submit complete reports, refer to Bug Hunter University. Note that only the first report of a specific vulnerability is rewarded.
- Bugs that are found in an SoC vendor's specific code are awarded based on the respective vendor-specific guidelines, severity, and reward amounts.
- Google encourages responsible disclosure, and we believe responsible disclosure is a two-way street; it's our duty to fix serious bugs within a reasonable time frame. Bugs initially disclosed publicly, or to a third-party for purposes other than fixing the bug, typically do not qualify for a reward.

There are also a few classes of vulnerabilities that generally do not qualify for a reward:

- Phishing attacks that involve tricking the user into entering credentials.
- Issues that only affect userdebug builds

- Issues with negligible security impact, as described in Bug Hunter University, with some exceptions.

Reward amounts

The reward amount depends on the severity of the vulnerability and the quality of the report. A valid, but low quality bug report may receive up to $200. Rewards are based on the severity and completeness of the report, and are up to the discretion of the rewards committee.

A complete report includes as much detail as possible, a proof of concept, a crash dump if available, and any additional repro steps. Additionally:

- It should reproduce on a recent build of Android, no older than 30 days from the time of submission.
- The proof of concept should be a complete Android Studio project, source code including an Android.bp file, or similar artifacts (e.g., a malformed media file or UX video walkthrough) depending on the context of the submitted vulnerability.
- Malformed files that are copyright material or can't be distributed with a CTS test may qualify for a lower reward amount.

Vulnerabilities which have different severities across the supported versions of Android are rewarded based on their severity on the most recent version of Android.

Patch submissions may qualify for a reward up to $1000 each. Patches should be submitted with the bug report or shortly thereafter. Patches submitted after a fix has been developed may not be eligible for rewards. The final amount is paid as per the discretion of the rewards committee. Submitted patches must apply cleanly to AOSP's master branch, comply with Coding Style Guidelines, and be accepted as the actual fix to be eligible for these additional reward amounts.

Even if a vulnerability was originally submitted to a third-party bug bounty program, researchers who submit a report including a proof of concept via the Android security rewards program may qualify for a $1000 bonus reward, if we do not already have a working proof of concept. To qualify for this bonus reward, researchers are required to provide the CVE ID showing that the issue was addressed in an Android Security Bulletin on an eligible device.

The final amount is always chosen at the discretion of the reward panel. In particular, we may decide to pay even more for unusually clever or severe vulnerabilities, decide that a single report actually constitutes multiple bugs, or that multiple reports are so closely related that they only warrant a single reward. We understand that some of you are not interested in money. We offer the option to donate your reward to an established charity. If you do so, we will double your donation (subject to our discretion). Any rewards that are unclaimed after 12 months are donated to a charity of our choosing.

Investigating and reporting bugs

All bugs should be reported using the vulnerability form (select the appropriate Android product in the **Bug Location** step). If you are submitting a patch, please attach the files to the bug report. Again, if your patch doesn't conform to Android's Coding Style Guidelines, we may reduce the reward amount. When investigating a vulnerability, please only ever target your own devices. Never attempt to access anyone else's data and do not engage in any activity that would be disruptive or damaging to your fellow users or to Google.

Note that we are only able to answer technical security vulnerability reports. Non-security bugs and queries about problems with your account should instead be directed to Google Help Centers.

Frequently asked questions

Q: How can I maximize the potential reward for my report?

A: To earn as much money as possible for your bug, include a high quality bug report, a buildable proof of concept (against a recent build, no older than 30 days at time of submission), and a patch. Ensure that your patch adheres to Android's Code Style Guidelines; we may lower the reward amount if the code requires a lot of fixing up before we can include it in the Android source tree. Proofs of concept submitted after an issue has already been assessed, or patches submitted after an issue has already been fixed are generally not eligible for rewards.

Q: Can I still receive a reward even if I don't submit a full working exploit?

A: Yes! Our program rewards issues that contain a complete report and a working proof of concept, even if a full working exploit is not provided. As reported in our blog, during the most recent full year of our rewards program, our average payout for these categories of issues was completeness of the report.

Q: How do I find out if my bug is eligible?

A: We'll let you know if your bug is eligible, and we'll let you know once the panel decides on a reward amount. We can't tell you if your bug will qualify before you give us the details.

Q: If the bug is classified as low, when will it be fixed and will a CVE ID be assigned ?

A: Low severity issues are generally addressed in the next major versions, instead of through our Monthly Security Bulletins. We generally do not assign CVEs for this severity level.

Q: If the bug is classified as moderate, when will it be fixed and will a CVE ID be assigned?

A: Moderate severity issues are generally addressed in the next major versions, instead of through our Monthly Security Bulletins. We assign CVEs for this severity level at the time of the next major release.

Q: What happens if I disclose the bug publicly before a fix is available?

A: Please read our stance on coordinated disclosure. In essence, our pledge to you is to respond promptly and fix bugs in a sensible timeframe — and in exchange, we ask for a reasonable advance notice. Reports that go against this principle usually do not qualify, but we will evaluate them on a case-by-case basis. Note that we pay out rewards before the bug has been fixed in many cases. If you disclose the bug after getting the reward, but without giving us a reasonable deadline for fixing the issue, you may not be eligible for future rewards.

Q: What do you consider a reasonable disclosure deadline?

A: Google's own Project Zero gives us a 90 day disclosure deadline when they report Android bugs. We think that's reasonable.

Q: Do I still qualify if I disclose the problem publicly once fixed?

Q: I wish to report an issue through a vulnerability broker / someone not you. Will my report still qualify for a reward?

A: We believe that it is against the spirit of the program to privately disclose the flaw to third parties for purposes other than actually fixing the bug. Consequently, such reports typically do not qualify.

Q: What if somebody else also found the same bug?

A: Only the first report of a given issue that we were previously unaware of is eligible. In the event of a duplicate submission, the earliest filed bug report in the bug tracker is considered the first report.

Q: What about bugs that are only present in other popular, non-Pixel devices?

A: If a bug does not affect the latest version of Android available on an eligible device currently for sale in the U.S. in the Google Store, it generally does not qualify for a reward.

Q: What about bugs in custom ROMs for eligible Pixel devices?

A: No, bugs in custom ROMS are not covered.

Q: What if a bug has already been reported but still affects the latest Android version available on a device currently for sale in the Google Store?

A: We would still request that you submit the report. We are usually only able to reward the first person who reports a bug to us, but will determine that on a case-by-case basis.

Q: For the purpose of exploit rewards, what is a "remote or proximal" attack vector?

A: A remote attack vector means that the exploit could be launched against a target without regard for the device's physical location. For example, the exploit could be triggered by visiting a web page, by opening an email, or receiving an SMS/MMS message. Proximal means that the exploit must be launched in close physical proximity to the device. For example, an attack involving a bug as if the exploit was launched from an app.

Q: For the purpose of exploit rewards, what is a "kernel compromise"?

A: We mean that the integrity of the kernel has been breached. This could be achieved with arbitrary code execution in the kernel or with arbitrary kernel writes — for example, to disable SELinux.

Q: What about bugs in third-party components?

A: These bugs are often eligible (e.g., image libraries, media libraries, compression libraries, etc.). Note that we assign the severity rating based on the impact to Android. Only bugs that can be manifest or exploited through Android are eligible. We're interested in rewarding any information that enables us to better protect our users. In the event of bugs in an external component, we are happy to take care of responsibly notifying other affected parties.

Q: Can you keep my identity confidential from the rest of the world?

A: Yes. If selected as the recipient of a reward, and you accept, we need your contact details in order to pay you. However, at your discretion and if you ask us before the bug is made public, we can credit the bug to "anonymous" and remove identifying information from the patch and bug entry.

Q: Can I submit my report now and provide a working exploit later? Is there a time limit for submitting an exploit?

A: When submitting a bug, please include steps to reproduce the issue and a working proof of concept to maximize your reward. We are willing to accept a fully working exploit a few weeks after the initial report. Exploits and proofs of concept submitted outside of this time frame are unlikely to be rewarded.

Q: Can I submit my report without having to create a Google account?

A: We would strongly prefer that report submissions take place through the vulnerability form.

this account can be encrypted using the Android Security PGP key.

Legal points

We are unable to issue rewards to individuals who are on sanctions lists, or who are in countries (e.g. Crimea, Cuba, Iran, North Korea, Sudan, and Syria) on sanctions lists. You are responsible for any tax implications depending on your country of residency and citizenship. There may be additional restrictions on your ability to enter depending upon your local law.

This is not a competition, but rather an experimental and discretionary rewards program. You should understand that we can cancel the program at any time and the decision as to whether or not to pay a reward has to be entirely at our discretion.

Of course, your testing must not violate any law, or disrupt or compromise any data that is not your own.

To avoid potential conflicts of interest, we will not grant rewards to people employed by Google or Google Partner companies who develop code for devices covered by this program.

Google Privacy Terms About Google Google Products Help